PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215167
(43)Date of publication of application : 04.08.2000

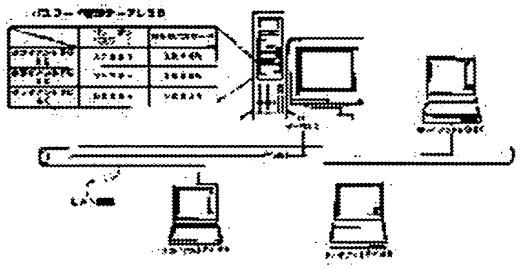
(51)Int.Cl. G06F 15/00
G06F 1/00

(21)Application number : 11-016461
(22)Date of filing : 26.01.1999

(71)Applicant : TOSHIBA CORP
(72)Inventor : UEHARA KEIICHI
MORISAWA SHUNICHI

(54) COMPUTER SYSTEM AND REMOTE CONTROL METHOD OF SAME SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To actualize remote management while maintaining the security of a client PC by allowing a server to send a password once receiving a request when sending a wake-up indication to the client PC.
SOLUTION: The server 10 sends a wake-up request to client PCs 20 to 40. The client PCs 20 to 40 judge that a security function is effectively set on condition that passwords are registered, and informs the server 10 of a password request. The server 10 reads the passwords corresponding to the client PCs out of a password management table 50 and informs the clients 20 to 40 of the read-out passwords to make requests to reset the passwords. The client PCs 20 to 40 performs a setting process for an instant security mode when the passwords from the server 10 match the registered passwords.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－215167
（P2000－215167A）
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
1/00	３７０	1/00	３７０Ｅ	

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－16461

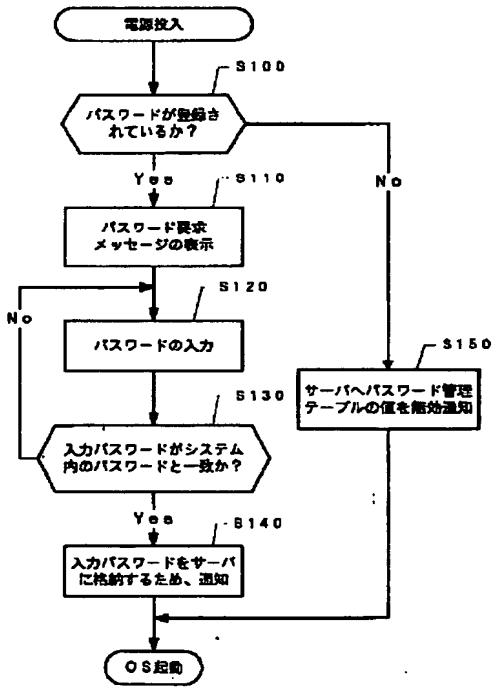
(22)出願日　平成11年１月26日(1999.1.26)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　上原　啓市
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(72)発明者　森沢　俊一
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100083161
弁理士　外川　英明

Ｆターム(参考)　5B085 AC02 AE03 BG07

(54)【発明の名称】　コンピュータシステム及びそのシステムのリモート制御方法

(57)【要約】
【課題】　十分なセキュリティを維持した状態でクライアントＰＣのリモート管理を実現する。
【解決手段】　ＰＣ本体やＨＤＤの様なセキュリティ機能を持つ装置に対して、電源オン操作の制御が行われた際、キーボード等から入力されたパスワードをサーバ内のパスワード管理テーブルに格納する。サーバは、セキュリティ機能を持つ装置をＷＯＬによりウェークアップ指示を送信する。サーバは、セキュリティ機能を持つ装置からパスワードの要求を受信すると、パスワード管理テーブルから対応するパスワードを読み出す。その後、サーバは、セキュリティ機能を持つ装置に対し、該パスワードを送信し、セキュリティ機能を持つ装置を通常の動作状態に復帰させる。



【特許請求の範囲】
【請求項１】　ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置と、
前記コンピュータ装置は、更に、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、
前記ネットワーク制御装置は、前記送信されたパスワードを記憶する手段を具備し、前記コンピュータ装置にウェークアップ指示を送信した時、前記コンピュータ装置からパスワードの要求を受信すると、前記記憶されたパスワードを読み出し、前記コンピュータ装置に対し、該パスワードを送信する手段とを具備することを特徴とするコンピュータシステム。
【請求項２】　前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする請求項１記載のコンピュータシステム。
【請求項３】　前記ネットワーク制御装置の記憶する手段は、パスワード管理テーブルから構成され、前記コンピュータ装置各々から送信されたパスワードを前記パスワード管理テーブルに格納する手段とを具備することを特徴とする請求項２記載のコンピュータシステム。
【請求項４】　前記コンピュータ装置は、電源オン操作の制御が行われた際、入力されたパスワードを格納する手段とを具備することを特徴とする請求項３記載のコンピュータシステム。
【請求項５】前記コンピュータ装置は、前記ネットワーク制御装置からパスワードを受信した時、前記コンピュータ装置内に格納されたパスワードを参照し、前記コンピュータ装置のセキュリティ機能を解除することを特徴とする請求項４記載のコンピュータシステム。
【請求項６】　ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータシステムに於いて、
前記コンピュータ装置は、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、
前記ネットワーク制御装置から前記コンピュータ装置にウェークアップ指示が送信された時、前記ネットワーク制御装置に対し、パスワード要求を送信する手段と、
パスワード要求を送信後、前記ネットワーク制御装置からパスワードを受信する手段とを具備することを特徴とするコンピュータシステム。
【請求項７】　前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする請求項６記載のコンピュータシステム。
【請求項８】　前記コンピュータ装置は、該コンピュータ装置の電源オン操作の制御が行われた際にパスワードが登録されていない場合、前記ネットワーク制御装置にパスワード消去・無効の要求を送信する手段とを具備することを特徴とする請求項７記載のコンピュータシステム。
【請求項９】　前記コンピュータ装置は、前記ネットワーク制御装置からパスワードを受信した時、前記コンピュータ装置内に格納されたパスワードを参照し、前記コンピュータ装置のセキュリティ機能を解除することを特徴とする請求項８記載のコンピュータシステム。
【請求項１０】　ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置で使用されるリモート制御方法に於いて、
前記コンピュータ装置は、更に、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信するステップと、
前記ネットワーク制御装置は、前記送信されたパスワードをパスワード管理テーブルに記録するステップと、
前記ネットワーク制御装置は、前記コンピュータ装置にウェークアップ指示を送信した時、前記コンピュータ装置からパスワードの要求を受信するステップと、
前記ネットワーク制御装置は、前記パスワード管理テーブルから前記パスワードを読み出し、前記コンピュータ装置に対し、該パスワードを送信するステップとを具備することを特徴とするコンピュータシステムのリモート制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コンピュータシステムのリモート制御に係わり、特に、サーバからの特定のパケット受信に応答して、停止状態、又は、スリープ状態のクライアントを通常動作状態に復帰するコンピュータシステムのリモート制御に関する。
【０００２】
【従来の技術】近年、企業内のパーソナルコンピュータ（ＰＣ）を集中管理するために、サーバから各ＰＣをリモート制御するためにＤｅｓｋｔｏｐ　Ｍａｎａｇｅｍｅｎｔ Ｉｎｔｅｒｆａｃｅ（ＤＭＩ）と称される標準インターフェース仕様に基づき、デスクトップＰＣの開発が行なわれている。
【０００３】上記ＤＭＩに基づき、サーバからのリモート制御でデスクトップＰＣを電源オンさせる「Ｗａｋｅ＿Ｏｎ＿ＬＡＮ（ＷＯＬ）」およびデスクトップＰＣの異常をサーバに自動的に通知する「Ａｌｅｒｔ＿Ｏｎ＿ＬＡＮ（ＡＯＬ）」と呼ばれる機能を搭載したデスクト

ップＰＣが製品化されている。

【０００４】ＷＯＬを用いた典型的なリモート管理の形態は、企業内の情報化ツールとして従業員各々の机上にデスクトップＰＣを配置し、これらをＬｏｃａｌ　ＡｒｅａＮｅｔｗｏｒｋ（ＬＡＮ）を介してサーバと結んだ動作環境とする。各デスクトップＰＣにインストールされているソフトウェアをバージョンアップする際や、各デスクトップＰＣからデータを収集する場合、サーバおよび従業員各々のデスクトップＰＣを管理する部門は、例えば、特定の日の退社時に各デスクトップＰＣをＷＯＬできる状態にして帰宅するように各従業員に求める。管理部門は、その深夜、サーバから特別なパケットを各デスクトップＰＣに送信し、電源オフ状態、又は、スリープ状態にある各デスクトップＰＣを自動的に立ち上げてソフトウェアのバージョンアップとデータ収集処理を行う。

【０００５】このようにサーバからのリモート制御で企業内の各デスクトップＰＣを集中管理することができる。通常、ＰＣ本体には、第三者による不正使用を防止するために、パワーオンパスワード機能が設けられている。このパワーオンパスワード機能に於いては、ＰＣ本体の電源投入時にＰＣのユーザによって入力されたパスワードをチェックし、所定のパスワードが入力された時にのみＰＣ本体のシステムを起動可能とする。このパスワード機能の有効／無効は、ユーザによるパワーオンパスワードの登録・登録解除操作などによって行われる。

【０００６】また、ＰＣには、第三者によるＨＤＤの不正抜取りによる使用を防止するために、アクセスロック機能が設けられている。このアクセスロック機能に於いて、オペレーティングシステム（ＯＳ）がＰＣのスリープ状態を管理する場合、自動的に、ＨＤＤに供給される電源がオフされるため、ＨＤＤに供給される電源オフにより、ＨＤＤはアクセスロック状態になる。ＨＤＤのアクセスロック状態の解除には、再度、ユーザは、ＨＤＤパスワードを入力する。このアクセスロック機能の有効／無効も、ユーザによるＨＤＤパスワードの登録・登録解除操作などによって行われる。

【０００７】上記パワーオンパスワード機能とアクセスロック機能が有効状態に設定されると、ＰＣ本体やＨＤＤに電源が投入されても正しいパスワードが入力されない限り、ＰＣのシステム状態は通常の動作状態に復帰されない。従って、ＰＣ本体が起動できず、ＨＤＤに格納された機密情報などが第三者に漏洩されるといった事態を防止できるので、ＰＣのセキュリティーを維持することができる。

【０００８】

【発明が解決しようとする課題】しかしながら、上記した従来技術では、ＰＣのパワーオンパスワード機能やアクセスロック機能を有効に設定してしまうと、今度は、ＷＯＬによるＰＣを夜間に電源オンしても、正当なパスワードを入力しない限り、ＰＣのシステム状態は通常の動作状態に復帰できない。この為、サーバからのリモート制御でクライアントＰＣを無人でスタートさせるというＷＯＬ本来の性能が損なわれてしまう。

【０００９】そこで、本発明は上記の問題を解決するためになされたものであり、クライアントＰＣの十分なセキュリティを維持した状態で、前述のリモート管理を実現することができるコンピュータシステム及びそのシステムのリモート制御方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】この発明は、ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置と、前記コンピュータ装置は、更に、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、前記ネットワーク制御装置は、前記送信されたパスワードを記憶する手段を具備し、前記コンピュータ装置にウェークアップ指示を送信した時、前記コンピュータ装置からパスワードの要求を受信すると、前記記憶されたパスワードを読み出し、前記コンピュータ装置に対し、該パスワードを送信する手段とを具備したことを特徴とする。

【００１１】また、本発明の前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする。このような構成によれば、クライアントＰＣの各種パスワード登録時、ネットワーク制御装置にも同じパスワードを管理・格納するので、ＷＯＬの為に、クライアントＰＣのパスワードを解除なしに、クライアントＰＣの十分なセキュリティを維持した状態で、リモート管理を実現することができる。

【００１２】また、本発明の前記ネットワーク制御装置の記録する手段は、パスワード管理テーブルであり、前記コンピュータ装置各々から送信されたパスワードを前記パスワード管理テーブルに格納する手段とを具備することを特徴とする。

【００１３】このような構成によれば、ネットワーク制御装置は、各種クライアントＰＣのパスワードを一元的に管理でき、クライアントＰＣのパスワードが、ユーザによって、登録・更新する度に、ネットワーク制御装置のパスワード管理テーブルの対応する箇所にクライアントＰＣのパスワードを更新できる。

【００１４】また、本発明のコンピュータ装置は、電源オン操作の制御が行われた際、入力されたパスワードを格納し、ネットワーク制御装置からパスワードを受信した時、コンピュータ装置内に格納されたパスワードを参照し、コンピュータ装置のセキュリティ機能を解除することを特徴とする。

【００１５】このような構成によれば、ネットワーク制御装置のパスワード管理テーブルから読み出されたパスワードをとコンピュータ装置のパスワードと容易に照合することが可能となる。

【００１６】更に、この発明は、ネットワークに接続され、ネットワーク制御装置から送信されるウェークアップ信号に応答して、動作状態に復帰するウェークアップ機能を持つコンピュータ装置に於いて、前記コンピュータ装置は、セキュリティ機能を具備し、該コンピュータ装置の電源オン操作の制御が行われた際、入力されたパスワードを前記ネットワーク制御装置に送信する手段と、前記ネットワーク制御装置から前記コンピュータ装置にウェークアップ指示が送信された時、前記ネットワーク制御装置に対し、パスワード要求を送信する手段と、パスワード要求を送信後、前記ネットワーク制御装置からパスワードを受信する手段とを具備することを特徴とする。

【００１７】また、本発明は、前記コンピュータ装置のセキュリティ機能は、パワーオンパスワード機能、又は、アクセスロック機能であることを特徴とする。このような構成によれば、パスワードが登録されているクライアントＰＣにおいて、ＷＯＬの為に、クライアントＰＣのパスワードを解除なしに、クライアントＰＣの十分なセキュリティを維持した状態で、リモート管理を実現することができる。

【００１８】また、更に、本発明のコンピュータ装置は、コンピュータ装置の電源オン操作の制御が行われた際、パスワードが登録されていない場合、前記ネットワーク制御装置にパスワード消去・無効の要求を送信する手段とを具備することを特徴とする。このような構成によれば、ネットワーク制御装置のパスワード管理テーブルを参照すれば、クライアントＰＣのセキュリティ機能を管理することができる。

【００１９】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図１には、本発明の一実施形態に係わるネットワークに接続された各コンピュータシステムが示されている。このコンピュータシステムは、Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（ＬＡＮ）上に接続されたサーバ１０と、複数のクライアントＰＣ２０～４０から構成されている。サーバ１０は、各クライアントＰＣ２０～４０間とのネットワーク管理および、ＤＭＩを介して、ネットワークに接続された各クライアントＰＣのリモート制御を行う。更に、サーバＰＣ１０は、ＷＯＬを利用して、各クライアントＰＣ２０～４０をリモート制御する為、各クライアントＰＣ２０～４０毎（ごと）のパスワードを管理するパスワード管理テーブル５０を具備している。このパスワード管理テーブル５０には、各クライアントＰＣ２０～４０毎のパワーオンパスワードとＨＤＤパスワード等のパスワードデータを格納する。サーバ１０は、パスワード管理テーブル５０に格納された各パスワードデータを読み出し、パワーオンパスワード機能およびアクセスロック機能を有する各クライアントＰＣ２０～４０のパスワードを解除し、ＷＯＬによる各クライアントＰＣ２０～４０にインストールされたソフトウェアをバージョンアップおよび各クライアントＰＣ２０～４０からのデータ収集を行う。

【００２０】図２には、本発明の一実施形態に係わるクライアントＰＣのシステム構成が示されている。このクライアントＰＣのシステムは、ノートブックタイプまたはサブノートタイプのポータブルパーソナルコンピュータである。ポータブルパーソナルコンピュータは、コンピュータ本体と、このコンピュータ本体に開閉自在に取り付けられたＬＣＤパネルユニットから構成されている。

【００２１】ポータブルパーソナルコンピュータ本体には、ＰＣＩバス、ＩＳＡバス、ＣＰＵモジュール６０、主メモリ７０、ＶＧＡコントローラ８０、ビデオメモリ（ＶＲＡＭ）９０、ＰＣＩインターフェイスブリッジ（ＰＣＩ　Ｉ／Ｆ）１００、Ｉ／Ｏコントローラ１１０、フロッピーディスクドライブ（ＦＤＤ）１２０、ハードディスクドライブ（ＨＤＤ）１３０、フラッシュＢＩＯＳ－ＲＯＭ１４０、キーボードコントローラ（ＫＢＣ）１６０、ＬＡＮコントローラ１７０などが設けられている。

【００２２】ＣＰＵモジュール６０は、このシステム全体の動作制御およびデータ処理を実行するものであり、ここにはＣＰＵ、キャッシュ、さらには主メモリ７０を制御するためのメモリコントローラなどが搭載されている。

【００２３】主メモリ７０は、このシステムの主記憶として使用されるものであり、オペレーティングシステム、処理対象のアプリケーションプログラム、およびアプリケーションプログラムによって構成されたユーザデータ等が格納されている。

【００２４】ＶＧＡコントローラ８０は、このシステムのディスプレイモニタとして使用されるＬＣＤおよび外部ＣＲＴを制御するためのものであり、ＶＲＡＭ９０に描画された画面データをそれらディスプレイモニタに表示する。

【００２５】ＰＣＩインターフェイスブリッジ（ＰＣＩ　Ｉ／Ｆ）１００は、１チップＬＳＩによって実現されたゲートアレイであり、ここには、ＰＣＩバスとＩＳＡバスとの間を双方向で接続するブリッジ機能が内蔵されているほか、ＨＤＤ１３０の制御を行うＩＤＥコントローラなども内蔵されている。

【００２６】Ｉ／Ｏコントローラ１１０は、各種Ｉ／Ｏデバイスを制御するためのゲートアレイであり、ＰＣＭＣＩＡ／ＣＡＲＤ　ＢＵＳ仕様のＰＣカードを制御する機能および、ＦＤＤ１２０を制御する機能の他、シリア

ルポート、パラレルポート、赤外線通信ポートなどの制御機能を有している。パワーオンパスワード登録時にＦＤＤ１２０にフロッピーディスク（ＦＤ）を装着しておくと、そのＦＤに登録パスワードが保存される。

【００２７】フラッシュＢＩＯＳ－ＲＯＭ１４０は、システムＢＩＯＳ（Ｂａｓｉｃ　Ｉ／Ｏ　Ｓｙｓｔｅｍ）を記憶するためのものであり、プログラム書き替えが可能なようにフラッシュメモリによって構成されている。システムＢＩＯＳは、このシステム内の各種ハードウェアをアクセスするためのファンクション実行ルーチンを体系化したものであり、ここには、パワーオンパスワードおよびＨＤＤパスワードおよびインスタントセキュリティなどの機能も含まれる。登録された各種パスワードは、フラッシュＢＩＯＳ－ＲＯＭ１４０内の所定の記憶領域であるパスワードブロック１５０に書き込まれる。

【００２８】フラッシュＢＩＯＳ－ＲＯＭ１４０内にパワーオンパスワードが登録されている場合には、システムがパワーオンされても、そのフラッシュＢＩＯＳ－ＲＯＭ１４０内に登録されているパスワードと同じパスワードが、キーボード（ＫＢ）操作によってユーザから入力されるまで、ＯＳの起動や、サスペンドモードからの復帰は禁止されている。

【００２９】また、システムのパワーオン、ハイバーネーションまたはサスペンドモード・レジュームからの復帰時でのＰＣのＨＤＤの電源供給時、システムＢＩＯＳは、ＨＤＤパスワードがＨＤＤ１３０内のＥＥＰＲＯＭに登録されている、即ち、ＨＤＤがアクセスロック状態であると判定した場合、ＨＤＤパスワードと同じパスワードが、キーボード（ＫＢ）操作によってユーザから入力されるまで、ＨＤＤへの読み出し・書き込みアクセスが禁止される。

【００３０】フラッシュＢＩＯＳ－ＲＯＭ１４０には、システム環境設定を変更するためのセットアッププログラムも格納されており、所定のキー操作を行うことによりそのセットアッププログラムを起動することができる。パワーオンパスワードおよびＨＤＤパスワード（以下、パスワードと称す）の登録および解除は、フラッシュＢＩＯＳ－ＲＯＭ１４０のセットアッププログラム、あるいは外部ＦＤなどによって供給されるセットアッププログラムを起動することによって行うことができる。

【００３１】フラッシュＢＩＯＳ－ＲＯＭ１４０あるいは外部ＦＤなどからセットアッププログラムを起動すると、システムセットアップメニュー画面が表示される。パスワードが登録されてない場合には、システムセットアップメニュー画面上のパスワードの設定項目「ＰＡＳＳＷＯＲＤ」には、「ＮＯＴ　Ｒｅｇｉｓｔｅｒｅｄ」と表示されている。システムセットアップメニュー画面上でパスワード設定項目「ＰＡＳＳＷＯＲＤ」にカーソルを合わせてスペースキーを押すことにより、パスワード登録を要求することがでる。入力可能なパスワードは、例えば、英数文字で１０桁までに制限されている。

【００３２】パスワードが入力された場合、再度、確認のためにパスワードの入力がユーザに要求される。ユーザによって再度入力されたパスワードが先に入力されたパスワードと一致すると、その入力パスワードがフラッシュＢＩＯＳ　ＲＯＭ１４０のパスワードブロック１５０およびＨＤＤ１３０のＥＥＰＲＯＭ内に保存される。これによって、ＰＣのシステムにパスワードが登録されたことになる。

【００３３】キーボードコントローラ（ＫＢＣ）１６０は、キーボード（ＫＢ）、およびポインティングスティック（ＰＳ）またはマウスなどのポインティングデバイスの制御を行う。

【００３４】ＬＡＮコントローラ１７０は、前述のＷＯＬ機能およびＡＯＬ機能に対応し、ＬＡＮ回線を介して他のクライアントＰＣ２０～４０およびサーバ１０と通信する。ＷＯＬ機能が、クライアントＰＣのセットアッププログラム上で有効に設定されている場合、ＬＡＮコントローラ１７０はＬＡＮ回線を介してサーバ１０から特定のパケットを介して受信した時、クライアントＰＣ本体２０～４０を自動的に電源オンするためのウェークアップ信号を発生する。また、クライアントＰＣ本体２０～４０でＡＯＬ機能が有効に設定されている場合、ＬＡＮコントローラ１７０はＬＡＮ回線を介してクライアントＰＣ本体２０～４０の異常等をサーバ１０に自動通知する。

【００３５】次に、図３を参照して、クライアントＰＣのパスワードをサーバのパスワード管理テーブルに登録する操作手順を説明する。クライアントＰＣがユーザ、又は、オーナーによってパワーオンされると、システムＢＩＯＳにより以下の処理が行われる。

【００３６】まず、フラッシュＢＩＯＳ－ＲＯＭ１４０のパスワードブロック１５０内にパスワードが存在するか否かを調べることにより、システム内にパスワードが登録されている状態であるか否かが判定される（ステップＳ１００）。パスワードブロック１５０内にパスワードが登録されている場合（ステップＳ１００のＹｅｓ）、システムＢＩＯＳは、クライアントＰＣのディスプレイ上にパワーオンパスワードやＨＤＤパスワードの入力要求メッセージを表示する（ステップＳ１１０）。

【００３７】システムＢＩＯＳはパスワードブロック１５０内にパスワードが登録されていないと判定した場合、サーバ１０にパスワード管理テーブルに格納されたパスワードデータを消去、又は、無効する様に通知後、クライアントＰＣのＨＤＤにインストールされたＯＳを起動する（ステップＳ１００のＮｏ→ステップＳ１５０）。サーバ１０は、クライアントＰＣからパスワード管理テーブル５０のパスワードデータを消去、又は、無効する通知を受信した時、各クライアントＰＣに対応するパスワードデータとして、例えば、「０００ｈ」を

示すパスワード未登録データを格納する。

【００３８】次に、クライアントＰＣのディスプレイ上にパワーオンパスワードやＨＤＤパスワードの入力要求メッセージが表示された場合、クライアントＰＣのユーザは、キーボードを利用して、パワーオンパスワードを入力する（ステップＳ１２０）。システムＢＩＯＳは、入力されたパワーオンパスワードとパスワードブロック１５０内の登録パスワードとの照合を行う（ステップＳ１３０）。入力されたパワーオンパスワードとパスワードブロック１５０内の登録パスワードが一致すれば（ステップＳ１３０のＹｅｓ）、システムＢＩＯＳはＬＡＮ回線を介してサーバ１０に入力されたパワーオンパスワードを通知する。サーバ１０は、クライアントＰＣから通知されたパワーオンパスワードをパスワード管理テーブル５０の所定位置に格納する（ステップＳ１４０）。

【００３９】上記パワーオンパスワードの入力・照合と同様に、クライアントＰＣの電源投入に伴うパスワード入力の時点で、クライアントＰＣのセットアッププログラムにより、ＨＤＤ１３０のＥＥＰＲＯＭに既に格納されているＨＤＤパスワードと入力されたＨＤＤパスワードを照合する（ステップ１３０）。システムＢＩＯＳは、入力されたＨＤＤパスワードとパスワードブロック１５０内の登録パスワードが一致すれば、入力されたＨＤＤパスワードをパスワードブロック１５０に格納し、サーバ１０に入力されたＨＤＤパスワードを通知する。サーバ１０は、クライアントＰＣから通知されたＨＤＤパスワードをパスワード管理テーブル５０の所定位置に格納する（ステップＳ１４０）。

【００４０】ＨＤＤパスワードもクライアントＰＣのセットアッププログラムの処理時点で、パワーオンパスワードと同様に、パスワードブロック１５０に格納することもできる。この場合、クライアントＰＣの電源投入時、ＨＤＤパスワードをパスワードブロック１５０に格納しないで、サーバ１０に通知するだけで良い。

【００４１】システムＢＩＯＳは、サーバ１０にパスワードを通知後、サーバ１０からパスワード登録通知を受信すると、クライアントＰＣのＯＳを起動する。また、システムＢＩＯＳは、パスワードブロック１５０に登録されているパスワードが入力されたパスワードと一致しないと判定した場合（ステップＳ１３０のＮｏ）、システムＢＩＯＳは再度パスワード入力画面をディスプレイ上に表示し、ユーザにパスワード入力を促す。システムＢＩＯＳはパスワード解除のための試行回数が所定値（例えば、３回）に達したと判断した場合、エラー処理、例えば、クライアントＰＣの電源をオフし、以降の操作を禁止する。

【００４２】図４には、サーバからクライアントＰＣのリモート制御処理の手順を示す。図５には、クライアントＰＣのウェークアップ制御処理の手順を示す。次に、図４と図５を参照して、クライアントＰＣがサーバからのＷＯＬによって電源オンされた場合、クライアントＰＣのセキュリティ状態を解除する手順を説明する。

【００４３】企業内の各従業員机上のクライアントＰＣ２０～４０にインストールされているソフトウェアをバージョンアップする際および、各クライアントＰＣ２０～４０のＨＤＤからデータを収集する場合、管理部門では特定の日の退社時に各クライアントＰＣをＷＯＬができる状態にして帰宅するように従業員に求める。その深夜、サーバ１０から特別なパケットを各クライアントＰＣ２０～４０に通知し、ウェークアップの要求を行う（ステップＳ２００）。

【００４４】各クライアントＰＣ２０～４０は、電源オンされた停止状態、又は、スリープ状態からウェークアップすると、システムＢＩＯＳは、まず、ウェークアップ要因をチェックする（ステップＳ３００）。システムＢＩＯＳは、ＬＡＮコントローラ１７０からのウェークアップ信号Ｗａｋｅ＿Ｕｐによるものであるか、通常の電源スイッチ操作によるものであるか判別する（ステップＳ３１０）。

【００４５】ＬＡＮコントローラ１７０からのウェークアップ信号Ｗａｋｅ＿Ｕｐによるウェークアップ要求であれば（ステップＳ４１０のＹｅｓ）、システムＢＩＯＳはパスワードブロック１５０内にパワーオンパスワードやＨＤＤパスワードなどのパスワードが登録されているか否かを調べる。登録されていれば、システムＢＩＯＳはパワーオンパスワードやＨＤＤパスワードのようなパスワードチェック（セキュリティ）機能が有効設定されていると判断し、ＬＡＮ回線を介して、サーバ１０にパワーオンパスワードやＨＤＤパスワードなどのパスワード要求を通知する（ステップＳ３２０）。

【００４６】また、ウェークアップ要因がユーザによる電源スイッチ操作であったならば、システムＢＩＯＳは図３記載のステップＳ１００以降の手順を実行する（ステップＳ３１０のＮｏ）。

【００４７】クライアントＰＣからパスワード要求を受信したサーバ１０は、ウェークアップ信号を通知したクライアントＰＣにパスワードが登録されていると判断する（ステップＳ２１０）。サーバ１０は、パスワード管理テーブル５０からクライアントＰＣに対応したパワーオンパスワードやＨＤＤパスワードなどの各種パスワードデータを読み出す（ステップ２１０のＹｅｓ～ステップＳ２２０）。

【００４８】サーバ１０は、パスワードを要求した各種クライアント２０～４０にＰＣパスワード管理テーブル５０から読み出されたパスワードを通知し、パスワード解除の要求を行う（ステップＳ２３０）。

【００４９】クライアントＰＣ２０～４０は、サーバ１０からパスワード解除の要求を受信すると、サーバ１０からのパスワードがクライアントＰＣのパスワードブロック１５０内の登録パスワードと一致するか否か判定す

る（ステップＳ３３０）。登録パスワードと一致する場合（ステップＳ３３０のＹｅｓ）、クライアントＰＣのシステムＢＩＯＳは、パスワード解除の成功をサーバ１０に通知する。その後、クライアントＰＣのシステムＢＩＯＳは、以下のようなインスタントセキュリティモードの設定処理を行う（ステップＳ３４０）。

【００５０】即ち、システムＢＩＯＳは、まず、ＫＢＣ１６０にキーロックコマンドを転送し、キーロックを指示する。このコマンドに応答して、ＫＢＣ１６０は、全ての入力デバイス、つまり、キーボード、外部キーボードおよびマウスをロックする。これにより、ＫＢＣ１６０による通常のキーコード送信は、行われない。次いで、システムＢＩＯＳは、ＬＣＤパネル内のバックライトを制御する回路にコマンドを転送し、ＬＣＤパネルなどのディスプレイモニターの表示画面をブランクさせる。この画面ブランクは、ＬＣＤパネルのバックライトを消灯することによって行うことが出来る。

【００５１】このように表示画面をブランクし、且つ、キーロックした状態で、システムＢＩＯＳは、サーバ１０にパスワード解除の成功を通知し、クライアントＰＣのサスペンド・ハイバーネーションからの復帰処理、あるいは、通常のＯＳの起動を行う。これにより、サーバ１０は、クライアントＰＣ２０～４０からパスワード解除の成功の通知を受信後（ステップＳ２４０のＹｅｓ）、ネットワークを介してクライアントＰＣ２０～４０をアクセスする。

【００５２】一方、システムＢＩＯＳは、サーバ１０からのパスワードが、クライアントＰＣのパスワードブロック１５０に登録されているパスワードと一致しないと判定した場合、サーバ１０に対しパスワード要求を通知する（ステップＳ３３０のＮｏ）。

【００５３】システムＢＩＯＳは、サーバ１０からパスワード解除要求に従い、サーバ１０から送付されたパスワードをパスワード解除試行の実行を所定回数後、パスワードブロック１５０内の登録されたパスワードと一致しなければ、サーバ１０にパスワード解除の不成立を通知する。

【００５４】サーバ１０は、パスワード解除の不成立を通知する受信後、エラー処理、例えば、ユーザがクライアントＰＣの電源スイッチ操作に伴う起動時、ＷＯＬエラーメッセージを通知する準備を行う（ステップＳ２４０のＮｏ）。

【００５５】また、サーバ１０が、ウェークアップ信号を通知したクライアントＰＣからパスワード要求を受信しなかったならば、クライアントＰＣにパスワードが登録されていないと判断し、クライアントＰＣのサスペンド・ハイバーネーションからの復帰処理、あるいは、ＯＳ起動後、クライアントＰＣのＨＤＤにアクセスを実行する（ステップＳ２１０のＮｏ）。

【００５６】本願発明の様な構成にするからこそ、システムＢＩＯＳのセットアップ処理によるパスワード登録後、クライアントＰＣの電源スイッチの操作に伴うユーザから入力されたパスワードの度毎に、サーバ１０に入力パスワードを通知し、パスワード管理テーブル１５０のパスワードデータを更新することができる。従って、クライアントＰＣのパスワードを常に最新のものとして、サーバ１０がクライアントＰＣのセキュリティ管理を維持しながらリモート制御できる。

【００５７】尚、本願発明の実施形態では、クライアントＰＣのシステムをノートブックタイプ、またはサブノートタイプのポータブルパーソナルコンピュータで示したが、同様に、デスクトップタイプのパーソナルコンピュータでもクライアントＰＣを構成できる。

【００５８】更に、本願発明の実施形態では、システムＢＩＯＳのセットアップ処理によるパスワード登録後、クライアントＰＣの電源スイッチの操作に伴うユーザから入力されたパスワードをサーバ１０に通知し、パスワード管理テーブルに格納しているが、システムＢＩＯＳのセットアップ処理によるパスワード登録時、パスワードをサーバ１０に通知し、パスワード管理テーブルに格納することもできる。

【００５９】また、上記実施形態では、クライアントＰＣ毎にネットワークパスワードが割り当てられているならば、クライアントＰＣの電源スイッチの操作時、ユーザが入力したネットワークパスワードをサーバ１０のパスワード管理テーブルに格納することも出来る。

【００６０】また、更に、上記実施形態では、サーバからクライアントＰＣのリモート制御で、サーバからクライアントＰＣにパスワードを送信する時、クライアントＰＣのパスワードブロックにパワーオンパスワードやＨＤＤパスワードなどの複数のパスワードデータが登録されていても、サーバから送信されたパスワードデータのうちのいずれか一つに一致するならば、クライアントＰＣはインスタントセキュリティ処理を実行することもできる。

【００６１】

【発明の効果】以上説明したように、この発明によれば、クライアントＰＣの十分なセキュリティを維持した状態で、サーバからのリモート管理を実現することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係わるネットワークに接続された各コンピュータシステムを示す図。

【図２】同実施形態に係わるクライアントＰＣのシステム構成を示すブロック図。

【図３】同実施形態のクライアントＰＣのパスワードをサーバのパスワード管理テーブルに登録する手順を示すフローチャート。

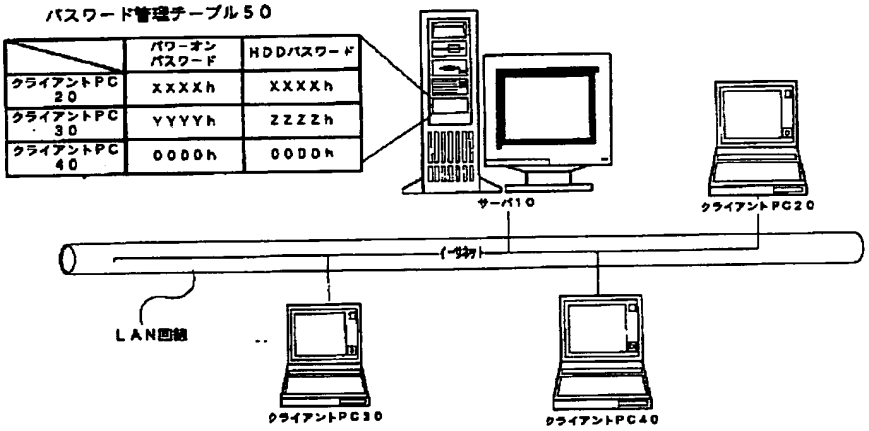
【図４】同実施形態のサーバからクライアントＰＣのリモート制御処理の手順を示すフローチャート。

【図５】同実施形態のクライアントＰＣのウェークアップ制御処理の手順を示すフローチャート。

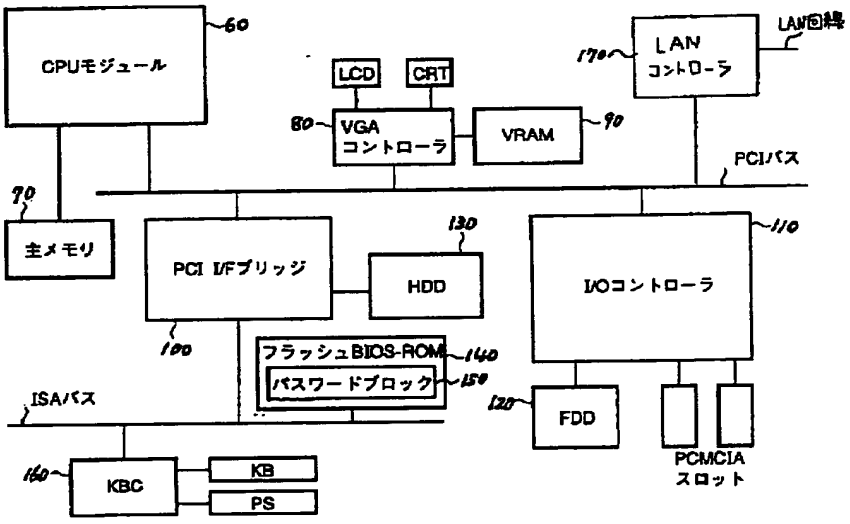
【符号の説明】

１０…サーバ、２０～４０…クライアントＰＣ、５０…パスワード管理テーブル、６０…ＣＰＵ、７０…主メモリ、８０…ＶＧＡコントローラ、９０…ＶＡＲＭ、１００…ＰＣＩインターフェースブリッジ装置、１１０…Ｉ／Ｏコントローラ、１２０…ＦＤＤ、１３０…ＨＤＤ、１４０…フラッシュＢＩＯＳ、１５０…パスワードブロック、１６０…ＫＢＣ、１７０…ＬＡＮコントローラ

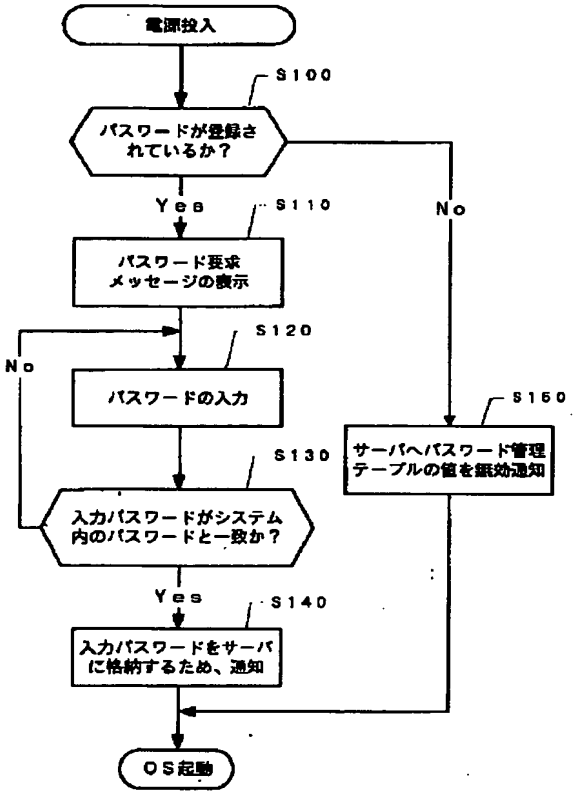
【図１】



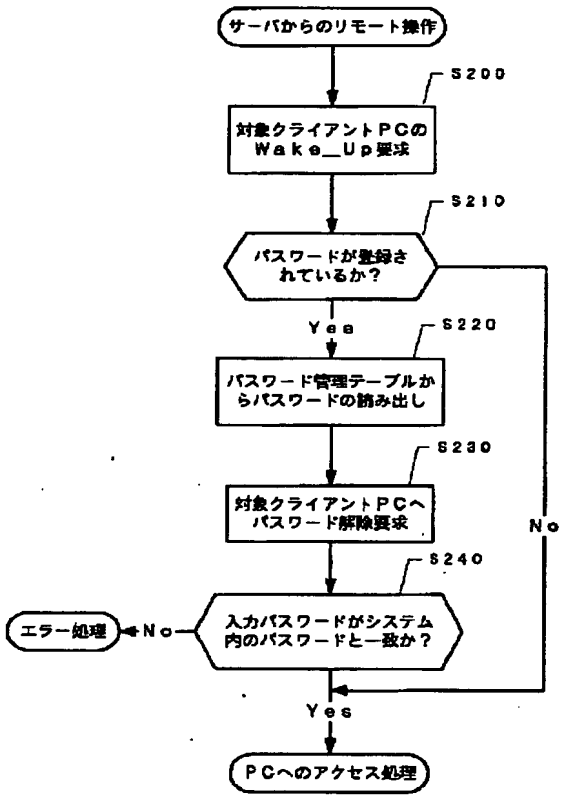
【図２】



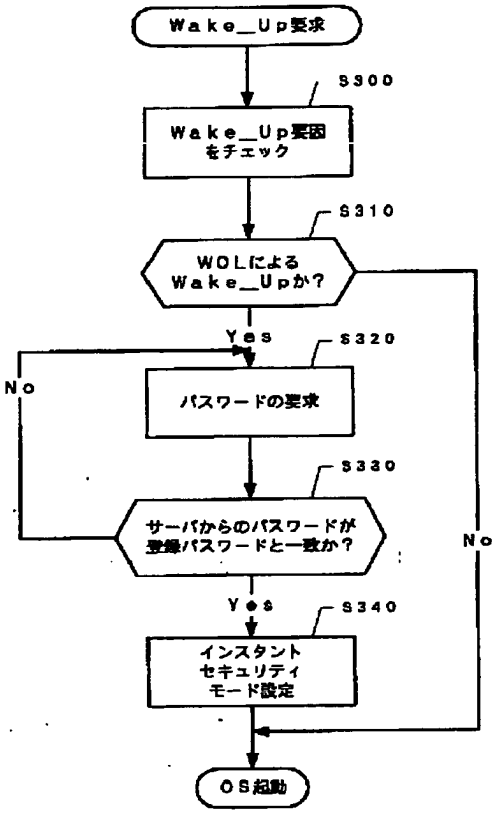
【図３】


電源投入
S100
パスワードが登録されているか？
Yes
No
S110
パスワード要求メッセージの表示
S120
No
パスワードの入力
S130
入力パスワードがシステム内のパスワードと一致か？
Yes
S140
入力パスワードをサーバに格納するため、通知
S150
サーバへパスワード管理テーブルの値を無効通知
OS起動

【図４】


サーバからのリモート操作
S200
対象クライアントPCのWake_Up要求
S210
パスワードが登録されているか？
Yes
No
S220
パスワード管理テーブルからパスワードの読み出し
S230
対象クライアントPCへパスワード解除要求
S240
エラー処理
No
入力パスワードがシステム内のパスワードと一致か？
Yes
PCへのアクセス処理

【図５】


Wake_Up要求
S300
Wake_Up要因をチェック
S310
WOLによるWake_Upか?
Yes
No
S320
パスワードの要求
S330
サーバからのパスワードが登録パスワードと一致か?
No
Yes
S340
インスタントセキュリティモード設定
OS起動